UNITED STATES DISTRICT COURT
DISTRICT OF PUERTO RICO

PABLO J. QUINTERO and JOANNIE PRINCIPE, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

METRO SANTURCE, INC., d/b/a PAVIA HOSPITAL SANTURCE, a corporation, METRO HATO REY, INC., d/b/a PAVIA HOSPITAL HATO REY and DOES 1 to 10, inclusive,

Defendants.

Case No.: 20-1075

MOTION TO DISMISS

Defendants Metro Santurce, Inc., d/b/a Pavia Hospital Santurce, a corporation, and Metro Hato Rey, Inc., d/b/a Pavia Hospital Hato Rey, a corporation, by and through their undersigned counsel and under Fed. R. Civ. P. 12(b)(1) and 12(b)(6) move to dismiss with prejudice the complaint filed by Pablo J. Quintero and Joannie Principe, individually and on behalf of all others similarly situated. Metro Pavía and Metro Hato Rey ("defendants") state as follows in support of their motion.

INTRODUCTION

Plaintiffs filed a putative class action complaint on February 11, 2020 seeking to recover damages arising out of an alleged security incident that happened on or about February 12, 2019 involving health/medical records maintained by defendants, which plaintiffs generically define as "PII." While the security incident occurred over a year ago, plaintiffs allege that their (and that of the putative class) PII was "exposed" and that they are at a "very high risk of identity theft and/or credit fraud . . . ." DE 1 at ¶¶ 4, 5,19. Further, while defendants offered plaintiffs twelve months

of complimentary credit monitoring and identity theft protection services, plaintiffs nevertheless allege that "they will be forced to incur the cost of a monitoring service . . ." as the security incident "placed them imminent, immediate and continuing risk of further theft-related harm." DE at ¶ 10.

Plaintiffs do not allege that the information they claim was compromised constitutes "personal health information" ("PHI")—the subject matter regulated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). They complain only that their ***PII*** was exposed. Even so, plaintiffs overlook that the causes of action they raise explicitly rest on HIPAA and the Federal Trade Commission Act ("FTCA"), neither of which confers private causes of action.

More importantly, plaintiffs do not allege that any PII was actually misused or that they otherwise experienced anything more than an apprehension of a potential risk of identity theft. This is significant as the security incident occurred over a year ago. Plaintiffs' complaint should be dismissed because they lack Article III standing and they otherwise fails to state a cognizable cause of action.

PLAINTIFFS' FACTUAL ALLEGATIONS

The following facts are draft from plaintiffs' complaint.

On February 12, 2019, Pavia Hospital Santurce (owned and operated by Metro Santurce) and the Pavia Hospital Hato Rey (owned and operated by Metro Hato Rey) experienced a security incident.[1] DE 1 at ¶ 1, 19. On June 18, 2019, defendants began notifying the patients whose information was involved in the incident. DE 1 at ¶ 20. The notification letters informed plaintiffs

[1] Defendants accept the allegations of the complaint for the limited purpose of the motion to dismiss, as required by law. Defendants reserve the right to challenge these allegations at a later time.

"[n]one of [their] information was lost as a result of the incident and to date there is no evidence to suggest that any of [their] information was exfiltrated from the network or that there has been any attempt to misuse [their] information." *See* Notification Letters to Plaintiffs, redacted and attached as **Group Exhibit A**.[2] Defendants nevertheless offered plaintiffs twelve months of complimentary credit monitoring and identity theft protection services. *Id.* Neither plaintiff alleges that he or she accepted the complimentary services.

Plaintiffs allege that defendants represented to their patients that they would protect their personal information and comply with HIPAA's privacy requirements. DE 1 at ¶ 21. As "covered entities" within the meaning of HIPAA, defendants were required to comply with HIPAA's Privacy Rule and Security Rule. DE 1 at ¶ 23. Defendants are likewise prohibited under the FTCA from engaging in unfair or deceptive practices, including the failure to maintain reasonable data security for consumers' personal information. DE 1 at ¶ 26.

Plaintiffs filed a putative class action complaint on February 11, 2020 seeking to recover damages they claim to have sustained from the February 12, 2019 incident. DE 1. Plaintiffs invoke federal jurisdiction under the Class Action Fairness Act ("CAFA") claiming diversity jurisdiction. DE 1 at ¶¶ 15-16. Plaintiffs allege that their PII was "exposed" during the incident, despite defendants' promises and representations to patients that this information would be protected. DE 1 at ¶ 21-22.

Plaintiffs also allege that defendants' respective websites include sections entitled "HIPAA Law" where defendants state that they will protect patients' private medical information. DE 1 at

[2] This Court may consider the notification letter even though it is not attached to the complaint because its authenticity is undisputed, it is referenced in the complaint, and it is central to Plaintiffs' claim. *Alternative Energy, Inc. v. St. Paul Fire & Marine Ins. Co*., 267 F.3d 30 (1st Cir. 2001); *Blue Ocean Int'; Bank LLC v. Golden Eagle Capital Advisors*, No. 19-1178, 2019 U.S. Dist. LEXIS 172977, n.1 (D.P.R. 2019).

¶21. Plaintiffs further allege that defendants are subject to HIPAA and references the various requirements of that statute as well as general standards of care and duties defendants owed with respect to plaintiffs' "protected health information." DE 1 at ¶¶ 23-25. But plaintiffs do not allege that the PII they claim was exposed in the incident was "protected health information." *Id*. Plaintiffs also allege that defendants were obligated under the FTCA from engaging in unfair or deceptive practices, which duty was breached as evidenced by the February 2019 incident. *Id*. at ¶¶ 26-32.

Plaintiffs further allege that the February 2019 security incident was a "data breach" that resulted in and will result in identity theft and identity fraud that costs billions of dollars because PII is valuable to thieves. DE 1 at ¶¶ 19-57. These allegations consist of a series of cites to websites, articles and include a flow chart. *Id*. Plaintiffs allege that defendants' failure to safeguard their information and the delayed notification of the February computer incident harmed them because they "have been placed at an imminent, immediate and continuing risk of harm from identity theft and identity fraud, requiring them to take the time and effort to mitigate the actual and potential impact" of the data breach by using preventative measures such as credit monitoring. DE 1 at ¶ 60-61. Plaintiffs nowhere allege that their information was actually used or misused by a third party. They also do not allege that they are actual victims of identity theft or identity fraud, only that they are at risk of becoming such a victim. *Id*.

Plaintiffs advance three theories of liability which they seek to pursue on a class basis: (1) breach of express and/or implied contract based on defendants' privacy notices on their websites; (2) breach of the covenant of good faith and fair dealing based on the same "contract" that was allegedly breached; and (3) negligence based on the alleged breach of duties defendants owed

under HIPAA, section 5 of the FTC Act and general failure to exercise reasonable care in handling patients' PII.

STANDARD

A. FRCP 12(b)(1)

A Rule 12(b)(1) motion challenges a court's subject matter jurisdiction. Fed. R. Civ. P. 12(b)(1); *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 89 (1998) (stating that a federal court has no subject matter jurisdiction absent Article III standing). The Constitution of the United States limits the subject matter jurisdiction of federal courts to actual cases and controversies. *Katz v. Pershing, LLC*, 672 F.3d 64, 71 (1st Cir. 2012), *citing* U.S. Const. Art. III, § 2). A court is powerless to hear a case where the plaintiff lacks Article III standing to pursue each asserted claim. *Katz*, 672 F.3d at 71, *citing Pagan v. Calderon*, 448 F.3d 16 (1st Cir. 2006).

B. FRCP 12(b)(6)

A motion under Rule 12(b)(6) challenges the legal sufficiency of the plaintiff's complaint. *Rosado-Montes v. United States*, 8 F. Supp. 3d 55 (D.P.R. Mar. 31, 2014). This Court accepts all of the well-pleaded allegations of the complaint as true and draws all reasonable inferences in favor of the plaintiff in considering such a motion. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007). To state a claim under the Federal Rules, a complaint need only contain "a short and plain statement of the claim showing that the pleader is entitled to relief." Fed. R. Civ. P. 8(a)(2). "[D]etailed factual allegations are not required, but the plaintiff must allege facts that when accepted as true . . . 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678, (2009) (quoting *Twombly*, 550 U.S. at 570). *See also Garcia-Catalan v. United States*, 734 F.3d 100, 102-03 (1st Cir. 2013) (stating that there must be more than a "sheer possibility" that a defendant acted unlawfully).

ARGUMENT

Plaintiffs lack standing because they suffered no injury—there is no allegation that their identities were actually stolen or that they actually suffered any manner of financial or other measurable harm. Plaintiffs suffered no damages because they lost nothing and their information was not misused. More importantly, plaintiffs cannot bring these claims in the first place because each is rooted in federal statutes—HIPPA and the FTCA—both of which explicitly preclude private causes of action. The complaint should be dismissed in its entirety and with prejudice.

I. PLAINTIFFS LACK STANDING BECAUSE THEY DID NOT SUFFER ANY CONCRETE, PARTICULARIZED INJURY.

Neither plaintiff has standing because neither suffered any actual injury. There is no allegation that either one actually had his or her identity stolen. The complaint instead says that their personal information was compromised, and that plaintiffs were placed at an "imminent, immediate, and continuing risk of harm." DE 1 at ¶¶ 60. These allegations concede the absence of any actual harm. As such, the question is whether the mere threat of a vague harm that has not materialized one year after the incident satisfies Article III standing. It does not.

Article III standing addresses whether the plaintiff has "such a personal stake in the outcome of the controversy as to assure that concrete adverseness which sharpens the presentation of issues upon which the court so largely depends for illumination." *Baker v. Carr*, 369 U.S. 186, 204 (1962). The plaintiff bears the burden to establish his or her own standing. *Hochendoner v. Genzyme Corp.*, 823 F.3d 724, 731 (1st Cir. 2016). *See also Spokeo Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016). To do so, they must establish each of three elements: injury, causation, and redressability. *Katz v. Pershing, LLC*, 672 F.3d 64, 71 (1st Cir. 2012). None are satisfied here.

A. The Plaintiffs suffered no injury in fact.

Standing requires demonstration of an injury-in-fact that is concrete, particularized and actual or imminent, not merely conjectural or hypothetical. *Barker v. Transp. Sec. Admin.*, 353 Fed. Appx. 450, 452 (1st Cir. 2009). It is not enough that harm might occur at some future time. *Katz*, 672 F.3d at 71, *citing Lujan v. Defs. of Wildlife*, 504 U.S. 555, 564, 112 S. Ct. 2130, 119 L. Ed. 2d 351 (1992). Plaintiffs are required to show that they were personally and actually injured, not merely that other unidentified members of the class to which they claim membership may have suffered an injury. *Spokeo,* 136 S. Ct. at 1548 n.6. A particularized injury must affect the plaintiff in a personal and individual way. *Spokeo,* 136 S. Ct. at 1548. A particularized injury alone is not sufficient, the injury must also be "concrete," meaning it must be real and not abstract. *Id*. The type of inchoate apprehension on which plaintiffs rely here is too speculative and remote to confer Article III standing. *See e.g., Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 414 (2013) (mere possibility of an injury insufficient to confer standing).

Although there is some dispute among circuits whether the threat of data misuse constitutes injury, the First Circuit (which controls here) held that it does not. *Katz*, 672 F. 3d at 80. The court in *Katz* addressed the issue presented here—whether a plaintiff who claims to be at an increased risk for identity theft, but is not an actual victim, satisfies the injury-in-fact requirement. 672 F.3d at 77-81. The plaintiff in that case alleged, among other things, that a defendant's failure to keep her non-public information secure caused an injury in fact because it increased risk of identity theft and the plaintiff had to take preventive measures to protect her identity. *Id*. at 78. The court nonetheless held that, without an identified misuse of the plaintiff's information, the plaintiff had no Article III standing. *Katz*, 672 F.3d at 79. The court also rejected the plaintiff's claims that her purchase of identity theft protection evidenced actual injury, reasoning that a choice to take action must be based on a reasonably impending threat as opposed to a theoretical

possibility. *Id*. at 79. *See also In re SuperValu, Inc*., 870 F.3d 763, 770 (8th Cir. 2017), and *Whalen v. Michaels Stores, Inc*., 689 F. App'x 89 (2d Cir. 2017) (unpublished) (also holding that mere apprehension is not injury-in-fact).

The allegations here mirror those in *Katz*: plaintiffs claim that the ***possibility of some future misuse of their identity*** and their purchase of identity monitoring constitute harm, despite making no claim that anyone actually misused identity information. The First Circuit addressed and dismissed these very claims in *Katz*. This Court should do the same.

Plaintiffs' entire complaint is based on an alleged security incident relating to her health/medical records in February 2019 which she judicially claims was impacted by a security incident "in which money was demanded in exchange for the release of the computer system." DE 1 at ¶19. While they also allege that PII was "exposed," neither alleges that their PII was actually used or misused by an unauthorized third party as the *Katz* court found was required. *Katz*, 672 F.3d at 80. Indeed, the sort of security incident alleged here does not involve the actual use or misuse of a person's PII. This much is confirmed by plaintiffs' reference to the demand for money to secure release of the system. DE 1 at ¶19.

Defendants aware of the circuit split where allegations of an increased risk of identity theft satisfy the injury-in-fact requirement of Article III. *See e.g., Galaria v. Nationwide Mut. Is. Co.*, 663 F. App'x 384, 388 (6th Cir. 2016) (unpublished); *Lewert v. P.F. Changs China Bistro, Inc*., 819 F.3d 963, 967 (7th Cir. 2016); and *In re Zappos.com, Inc*., 888 F.3d 1020, 1023 (9th Cir. 2018) (all finding injury in fact based on increased risk allegations). The Third and Fourth Circuits find standing exists depending on the facts pled. *Hutton v. Nat'l Bd. of Examiners in Optemetry, Inc*., 892 F.3d 613, 622 (4th Cir. 2018) (injury in fact); *Beck v. McDonald*, 848 F. 3d 262 (4th Cir. 2017) (no injury in fact); *In re Horizon Healthcare Services, Inc. v. Data Breach Litigation*, 846 F.3d

6235 (3d Cir. 2017) (injury in fact) and *Reilly v. Ceridian Corp*., 664 F.3d 38 (3d Cir. 2011) (no injury in fact).

But even though the case law on this question varies from circuit to circuit, it is the facts and circumstances pled in each case that drove the analysis. *See In re SuperValu, Inc*., 870 F.3d at 769 (different results turned on substance of allegations). This is to be expected given the factually intensive nature of the Article III standing analysis. Even so, at least one court considered the varied rulings and noted three common factors considered in determining whether a plaintiff exposed to an increased risk of identity theft (as is claimed here) suffered an injury in fact: (1) the motive of the unauthorized third party; (2) the type of data that was allegedly compromised; and (3) whether the third party already used the compromised data fraudulently. *In re 21st Century Oncology Customer Data Sec. Breach Litig*., No. 16-2737, 380 F. Supp.3d 1243, 1251-1255 (M.D. Fla. Mar. 11, 2019). The *In re 21st Century* court's application of these factors is instructive.

The plaintiffs in *In re 21st Century* alleged that their PII was actually used by third parties—it was being offered for sale. The data that was compromised included names, social security numbers, doctor's names, medical diagnoses and insurance information. The court found that there was an injury in fact because the hacker's intent was to specifically target the plaintiffs' PII, the data that was disclosed is the type used to commit identity theft and the data was actually accessed which was evidenced by the fact that it was offered for sale. *In re 21st Century*, 380 F. Supp.3d at 1255-1256. Applying each of these factors here leads to the conclusion that plaintiffs lacks standing.

The alleged bad actor's motivation here is gleaned from plaintiffs' judicial admissions. They allege that there was a "computer hack," the purpose of which was to encrypt defendants'

systems so that it could not be accessed until a payment was made.[3] DE 1 at ¶ 19. There is no allegation that the alleged unknown actors specifically targeted plaintiffs' (or anyone else's) PII to be able to use that information fraudulently. This omission is dispositive. *Khan v. Children's National Health System,* 188 F. Supp. 3d 524, 530 (D. Md. 2016) (finding no standing where the plaintiff's threat of future injury assumed that hackers read, copied, and understood the personal information; intended 'to commit future criminal acts by misusing the information; and used that information to the plaintiffs' detriment). Per plaintiffs, the goal here was to cripple defendants' operations until the requested payment was made. This factor weighs against finding an injury in fact. Defendants note that plaintiffs include a throwaway assertion that "Hackers do not target PII without the intent to use it fraudulently." DE 1 at ¶¶ 80; 90; 115. This assumption does not change the analysis.

The second factor—the type of information allegedly compromised—also weighs against finding an injury-in-fact. While it is true that the theft of PII is generally viewed as creating a material risk (*In re 21st Century*, 380 F.Supp3d at 1253), the nature of the information itself is not dispositive—it merely plays a role in the analysis. *Id*. The nature of the PII here admittedly includes social security numbers and other data points that can potentially be used to commit identity theft. But, as noted above, plaintiffs' PII itself was not compromised—it was merely caught up in an incident that impacted defendants' network. The notification letter that plaintiffs received makes clear that none of plaintiffs PII was misused. As such, the role this factor plays in the standing analysis is minimal.

Finally, there is no allegation that plaintiffs' PII was actually misused by any third party actor or that either plaintiff suffered any identity theft and/or credit fraud related to the incident.

[3] Defendants draw this conclusion for purposes of this motion only.

Plaintiffs instead cite to a litany of articles and websites that bemoan the evils of data breaches in general and the plight faced by those whose identity is actually misused by an unauthorized third party. DE 1 at ¶¶ 19-57. But simply because there are other instances where personal data is ***actually*** stolen and misused for fraudulent purposes does not mean that this happened here. Indeed, there is no indication—over one year later—that anyone accessed plaintiffs' PII, much less misused or sold it. Puerto Rico's own statute of limitations for negligence claims is one year. P.R. Laws Ann. tit. 31, § 5298. Certainly, if the entire statutory period has run without any evidence that the plaintiffs' information was misused, then the threat of harm cannot credibly be called "imminent."

Plaintiffs' claims are instead too speculative and hypothetical qualify as an injury-in-fact. *See In re Science Applications Intl Corp. Backup Tape Data Theft Litig. (SAIC)*, 45 F. Supp. 3d 14, 19 (D.D.C. 2014) (finding standing only as to individual plaintiffs who alleged actual misuse of their personal data); and *Green v. eBay Inc.*, No . Civ.A. 14-1688, 2015 U.S. Dist. LEXIS 58047 (E.D. La. May 4, 2015) (finding no standing where hackers accessed eBay's files containing users' personal information).

B. The Causation Criterion is not Satisfied.

The above discussion makes clear that plaintiffs do not allege facts to establish an injury in fact which is dispositive. Even if the Court were to consider causation, that element fails too.

The causation element requires plaintiffs to show a direct causal connection between the challenged action and the alleged harm. *Katz*, 672 F. 3d at 71. Plaintiffs claim that they were injured by the unauthorized third parties allegedly interfering with defendants' systems. The causal connection is absent because the harm (if any) was caused by the independent acts of a third party. *Id*.

C. Plaintiffs Seek to Redress a General Grievance at Best.

Plaintiffs are required to show that a favorable resolution will redress their claimed injury. *Katz*, 672 F. 3d at 72. The extensive citations to websites, articles and studies in the complaint shows that plaintiffs seek redress for the general adverse impacts of identity theft overall as opposed to an injury specific to them. This is because neither plaintiff suffered an injury specific to them.

D. Plaintiffs Lack Statutory Standing.

Woven throughout the complaint are allegations that defendants are subject to HIPAA and that they failed to comply with HIPAA's various rules and regulations, thereby compromising plaintiffs' PII. To the extent that plaintiffs rely on these allegations to satisfy Article III standing, that reliance is misplaced.

More importantly, while plaintiffs base the above allegations under HIPAA, she continuously refers to PII, which is not governed by HIPAA. HIPAA regulates PHI only. 45 CFR 164.501. By contrast, as a Puerto Rico resident plaintiffs' PII would be subject to Puerto Rico law, which is nowhere alleged in the complaint. 10 L.P.R.A. § 4051. To the extent that the Puerto Rico statute also encompasses PHI, HIPAA preemption applies. 45 C.F.R. § 160.203(b). Further, it is well settled that there is no private right of action under HIPAA. *Rosado-Montes v. United States*, 8 F. Supp. 3d 55, 58 (D.P.R. 2014) (noting the lack of a private right of action; HIPAA only enforceable through agency action). *Accord Federal Election Comm'n v. Akins*, 118 S. Ct. 1777, 20-25 (1998). As such, plaintiffs' allegations can only relate to claims under HIPAA for which no private right of action exists.

The lack of standing is dispositive and compels dismissal of plaintiffs' complaint in its entirety and with prejudice.

II. PLAINTIFFS SUFFERED NO DAMAGES.

The fact that the plaintiffs suffered no injury-in-fact is dispositive. Even so, the lack of standing also means they suffered no damages. The complaint alleges in paragraph 61 five general sources of damage, none of which meets the plausibility standard announced in *Iqbal* and *Twombly*:

a. *The improper disclosure, compromising, and theft of their PII.* As discussed at length in Part I, the mere specter that plaintiffs *might* suffer harm from the possible disclosure of their PII at some indeterminate point in the future is not a basis for damages. Moreover, the complaint assumes in this subparagraph, without any allegation elsewhere, that plaintiffs' PII was actually stolen. Actual theft would have been alleged. Factual allegations must rise above a speculative level to sustain a claim. *Twombly* at 555.

b. *The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of an unauthorized third-party and misused via the sale of Plaintiffs' and Class Members' information on the black market*. Characterizing any injury as "certain" and "impending" does not make it so. *Twombly* at 555. It has been over a year since the incident, and neither plaintiff alleged any misuse of their PII whatsoever. Allegations regarding sale of the plaintiffs' data or the black market are likewise entirely unfounded and unsupported speculation. The notification plaintiffs expressly states that the investigation by the defendants revealed no evidence that plaintiffs' information was exfiltrated from the network, nor any evidence that their information was misused.

c. *The untimely and inadequate notification of the data breach.* Plaintiffs do not allege how they were damaged by the notification. There is no allegation that they suffered identity theft (or anything like it) before receiving notification, nor is there any indication that they enrolled in credit monitoring at any point in the past year. To the contrary, the notification offered free credit

monitoring and identity theft recovery services, and plaintiffs never enrolled for either service. Plaintiffs behaved exactly the same after the notification as they did before.

d. *Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the data breach.* Plaintiffs identified no single expense incurred in responding to the notification from defendants. Moreover, the notification letter on which plaintiffs' claim is premised shows that they did not in fact have to spend any money redressing the incident. Defendants alerted plaintiffs in their notice that the defendants were offering twelve months of credit monitoring and identity theft recovery services at no charge to them. *See* Group Ex. A. Neither plaintiff enrolled in the free credit monitoring program.

e. *Ascertainable losses in the form of deprivation of the value of [the Plaintiffs'] PII, for which there is a well-established national and international market.* This allegation, like all those preceding it, substitutes generalizations about what happened in select and *unrelated* instances of identity theft as if those generalizations happened here. There is no support for any suggestion that anyone stole plaintiffs' PII, or that the PII lost its value.

In sum, each of plaintiffs' alleged damages suffers from the same defect: it assumes facts for which there is no support or supportable allegation. *Twombly* holds that the facts must create more than suspicion of what transpired. 550 U.S. at 555. The claim here could not be less concrete—it is based on a mistaken belief that their information was obtained by ill motivated third parties and a hunch that the information will be misused in the future. That is insufficient. Plaintiffs cannot establish damages without some showing that someone actually misused their information. *See, e.g., Green v. eBay Inc.*, 2015 U.S. Dist. LEXIS 58047 (E.D. La. 2015). Alleged damages in a complaint need not be pleaded with specificity, but they cannot merely be

speculative. *See, e.g., Kelley v. Airborne Freight Corp.*, 140 F. 3d 335, 354 (1st Cir. 1998); *San Carlos Irrigation & Drainage Dist. v. United States*, 111 F. 3d 1557, 1563 (Fed. Cir. 1997); *Suitt Constr. Co. v. Ripley's Aquarium, LLC*, 108 Fed. Appx. 309, 314 (6th Cir. 2004). Dismissal of the complaint with prejudice is proper.

III. THE COMPLAINT OTHERWISE FAILS TO STATE A CLAIM.

The Court need not reach this issue if it agrees that plaintiffs lack standing. Even if the Court were to consider this question, the complaint is still subject to dismissal for failure to state a claim.

A. Any state law claims are preempted by HIPAA.

As a threshold matter, and as introduced above, to the extent there is an attempt to enforce HIPAA obligations relative to plaintiffs' PII (as opposed to PHI) under Puerto Rico law, that claim is preempted by HIPAA. 45 CFR § 160.202.

The Supremacy Clause of Article VI of the Constitution provides Congress with the power to preempt state law. *Nat'l Ass'n of State Util. Consumer Advocates v. FCC*, 457 F.3d 1238, 1251 (11th Cir. 2006). HIPPA provides that provisions of state law which are contrary to HIPPA are preempted unless that state law is "more stringent." 45 C.F.R. §160.203. *See also* 42 U.S.C. § 1320d-7. "The Privacy Rule provides a floor of privacy protection. State laws that are more stringent remain in force." 67 Fed. Reg. 53182, 53212 (August, 14, 2002). More stringent means "with respect to a use or disclosure, the law prohibits or restricts a use or disclosure in circumstances under which such use or disclosure otherwise would be permitted." 45 C.F.R. § 160.202. The Puerto Rico law that protects PII is not more stringent than HIPPA.

The Citizen Information of Data Banks Security Act sets out the protections for a Puerto Rican citizen's "personal information file" which is defined to include the "medical information protected by HIPPA." *See* §4501(a)(5). The statute requires custodians of a "personal information

file" to notify Puerto Rican citizens of any violation of the security of their files. *See* §4502. The Puerto Rico statute does not include the heightened privacy requirements imposed by HIPPA and is preempted.

B. Plaintiffs Do Not Allege a Viable Breach of Either an Express or Implied Contract.

In an effort to avoid the obvious hurdle created by the lack of a private right of action under HIPAA (and ignoring the fact that PII is not governed thereunder), plaintiffs advance a breach of contract theory—both express and implied. But these theories fail because the "contract" plaintiffs claim was breached is an agreement to comply with HIPAA, as expressed in the privacy notices in the websites, and qualifies as a *de facto* effort to privately enforce HIPAA which is not recognized.

1. Plaintiffs Do Not Allege Breach of an Express Contract

The elements of a breach of contract in Puerto Rico are (1) a valid contract; (2) material breach; and (3) damages. *Mega Media Holdings, Inc. v. Aerco Broad Corp*., 852 F. Supp. 2d 189, 199 (D.P.R. 2012). A valid contract has three components under Puerto Rican law: (1) consent of the contracting parties; (2) a definitive legal object of the contract; and (3) consideration. *Id*. at 200.

The alleged contractual terms cited by plaintiffs are merely the provisions of HIPAA to which defendants are legally bound. Neither compliance with HIPAA obligations nor notice to patients of those obligations creates a contract. *Brush v. Miami Beach Healthcare Grp. Ltd.*, 238 F. Supp. 3d 1359, 1367 (S.D. Fla. 2017) (finding that notice to a patient of her privacy rights and the healthcare provider's obligations is not contractual in nature). HIPAA provisions require compliance regardless of whether defendants receive consideration, so they cannot create contractual obligations. *Weinberg v. Advanced Data Processing, Inc*. 147 F. Supp. 3d 1359 (S.D.

Fla. 2015). Privacy statements themselves do not create contractual obligations. *See, e.g., Abdale v. North Shore-Long Island Jewish Health System, Inc.*, 19 N.Y.S.3d 850, 859-60 (N.Y. Sup. Ct.).

Invocation of the common law breach of contract theory is not novel and is routinely rejected as an attempt to circumvent Congress' intent not to create a private right of action under HIPAA. *See e.g.*, *Cairel v. Jessamine Cty. Fiscal Court*, No. 15-186-JMH, 2015 U.S. Dist. LEXIS 167714 (E.D. Ky. Dec. 15, 2015) (a plaintiff cannot characterize HIPAA violation as breach of contract).

Try as they might, plaintiffs cannot manipulate common law to create a right of action where none exists. *Astra USA, Inc. v. Santa Clara Cnty., Cal.*, 563 U.S. 110, 118 (2011) (a suit to enforce a contract incorporating statutory obligations is in essence a suit to enforce the statute itself). Courts consistently rejected attempts to characterize alleged HIPAA violations as breaches of contract. The U.S. Supreme Court has also held more generally that a suit incorporating statutory obligations into a contract is in essence just a suit to enforce the contract itself. *Astra USA, Inc. v. Santa Clara Cnty., Cal.*, 563 U.S. 110, 118 (2011). Because HIPAA provides no private right of action, plaintiffs cannot sue for alleged HIPAA violations, no matter how the theory is crafted.

Plaintiffs likewise purport to premise a breach of contract under the FTCA, which likewise does not permit private causes of action.[4] *Tanol Distributors, Inc. v. Panasonic Co., Div. of Mastushita Electric Corp.*, 1987 U.S. Dist. LEXIS 15340 at 5 (Dist. Mass. 1987). *See also Jeter v. Credit Bureau, Inc.*, 760 F.2d 1168, 1174 n.5 (11th Cir. 1985); *Dreisbach v. Murphy*, 658 F.2d 720, 730 (9th Cir. 1981); *Fulton v. Hecht*, 580 F.2d 1243, 1249 n.2 (5th Cir. 1978), *cert. denied*,

[4] Plaintiffs themselves acknowledge that it is the FTC that brings enforcement actions against businesses for failure to protect customer information. *See* DE 1 at ¶ 30.

440 U.S. 981 (1979); *Holloway v. Bristol-Myers Corporation*, 485 F.2d 986 (D.C. Cir. 1973). Any allegations based on FTCA violations undermine, rather than underscore, plaintiffs' position. They cannot sue for FTCA violations, no matter how they style their claim.

2. There is No Breach of an Implied Contract

The above discussion makes clear that plaintiffs may not premise a breach of contract claim on alleged HIPAA violations with respect to PII. The same is true for the vaguely pled implied breach of contract theory. Plaintiffs cannot manipulate common law causes of action to manufacture a private right of action that Congress did not see fit to create. *Astra, supra*.

C. Plaintiffs Fail to State a Claim for the Breach of the Covenant of Good Faith and Fair Dealing.

Plaintiffs state no viable claim for breach of the covenant of good faith and fair dealing, both because there was no contract in the first place and because, even if there were a contract, a claim for the breach of the covenant of good faith requires a showing that defendants took some action in order to gain the fruits of the contract at plaintiffs' expense. Plaintiffs make the common mistake of tacking a breach of the covenant of good faith claim on to the back of a breach of contract claim, but the two are distinct and contain different elements. *See Artuso v. Vertex Pharms., Inc*., 637 F.3d 1 (1st Cir. 2011) (claims for the breach of the covenant of good faith and fair dealing are frequently used to bolster weak contract claims, but a breach of contract and breach of the covenant of good faith are distinct and must be treated as such).

1. There is No Breach of the Duty of Good Faith and Fair Dealing Absent a Contract.

As discussed above, there was no contract between defendants and plaintiffs. The breach of the implied duty of good faith and fair dealing 'is merely a breach of the underlying contract.'" *Fero v. Excellus Health Plan, Inc.*, 236 F. Supp. 3d 735, 762 (W.D.N.Y. 2017). Where there is no contract, there is no breach of the covenant of good faith and fair-dealing. *Mass. Eye & Ear*

Infirmary v. QLT Phototherapeutics, Inc., 412 F. 3d 215, 230 (1st Cir. 2005); *Accusoft Corp. v. Palo*, 237 F.3d 31, 45 (D. P.R. 2001). That fact alone is dispositive. But even if there were a contract, plaintiffs stated no viable claim for breach of the covenant of good faith because the complaint lacks any allegation that defendants acted in bad faith at any point. The complaint confuses bad faith and negligence, but they are not the same.

2. Negligent Conduct is not Bad Faith.

The covenant of good faith and fair dealing provides that "neither party shall do anything that will have the effect of destroying or injuring the right of the other party *to receive the fruits of the contract*." *See Accusoft Corp. v. Palo*, 237 F.3d 31 (D. P.R. 2001) (emphasis added). Although "bad faith" is subjective, a complaint requires more than mere speculation of improper conduct to survive a motion to dismiss. *Artuso,* 637 F.3d at 9. Because this complaint contains no specific allegations of bad-faith conduct, the Court may infer that the plaintiff is merely speculating, and should dismiss the claim. *Id.*

Put differently, plaintiffs must allege that defendants took some action in bad faith to state a claim for breach of the covenant. For example, in *Federal Deposit Ins. Corp. v. CNA Casualty of Puerto Rico*, this Court ruled that the FDIC could bring an action for breach of the covenant of good faith when the FDIC alleged that a bank president committed dishonest and fraudulent actions that cost a contract party $9 million. 786 F. Supp. 1082 (D.P.R. 1991). The Court elaborated that "dishonest" and "fraudulent" require some willful act by the defendant, and that mere negligence or error is insufficient.[5] *Id.* at 1087.

[5] The Court in this instance was analyzing the meaning of "fraudulent" with the context of a fidelity bond, but the analysis is applicable to the larger context of a breach of the covenant of good faith generally.

By contrast, defendants conduct here is at best characterized as negligent and is not the kind of conduct that justifies a claim for breach of the covenant of good faith. The claim should be dismissed with prejudice.

D. The Negligence Claim is a Thinly Veiled End Run Around the Lack of a Private Right of Action under HIPAA.

The same analysis that compels dismissal of the breach of contract theories applies here—there is no private right of action under HIPAA so an alleged violation of that statute cannot form the predicate of a negligence claim. Courts consistently hold that plaintiffs cannot sustain a negligence claim based on an alleged failure to comply with HIPAA. *Valentine-Munoz v. Island Fin. Corp.*, 364 F.Supp.2d 131, 136 (D. P.R. 2005) (collecting cases). HIPAA specifically states that only the Secretary of Health and Human Services or other state authority may bring a HIPAA enforcement action. *Id.*

Moreover, the Plaintiffs suggest that the failure to comply with the statutes is negligence *per se*. That is not so in instances, such as this one, where the statute forecloses a private right of action. *See Nerviano v. Contract Analysis Sys., LLC*, No. 17-4907, 2018 U.S. Dist. LEXIS 82253 (E.D. Penn. 2018) (dismissing a negligence claim premised on HIPAA violation because HIPAA provides no private right of action); *Haywood v. Novartis Pharms. Corp.*, 298 F. Supp.3d 1180, 1190-1191 (N.D. Ind. 2018) (stating that a HIPAA violation cannot be shoehorned into a negligence cause of action); and *Sheldon v. Kettering Health Network*, 2015 Ohio 3268, 40 N.E.3d 661, 672 (Ohio App. 2d Dist. 2015) (stating that using HIPPA as a predicate for an ordinary negligence claim is tantamount to private enforcement of that statute).

Finally, as discussed in Section C, *supra*, the FTCA likewise prohibits private causes of action, so plaintiffs likewise cannot premise a negligence claim on allegations complaining of FTCA violations.

The complaint should be dismissed in its entirety and with prejudice.

CONCLUSION

WHEREFORE, for the foregoing reasons, Metro Santurce, Inc. and Metro Hato Rey, Inc. respectfully request that this Court dismiss the complaint in its entirety and with prejudice.

Dated: May 13, 2020

Respectully submitted,

/s/ *Cinthia Granados Motley*
Cinthia Granados Motley *pro hac vice*
cmotley@dykema.com
DYKEMA GOSSETT PLLC
10 S. Wacker Drive, Suite 2300
Chicago, Illinois 60606
(312) 876-1700

/s/ Alberto G. Estrella
Alberto Estrella (USDC-PR 209804)
agestrella@estrellallc.com
ESTRELLA, LLC
P.O. Box 9023596
San Juan, Puerto Rico 00902–3596
Tel.: (787) 977-5050 Fax: (787) 977-5090

Attorneys for Defendants Metro Santurce, Inc. and Metro Hato Rey, Inc.

CERTIFICATE OF SERVICE

I hereby certify that on this date, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification to the parties of record.

/s/Alberto G. Estrella
Alberto G. Estrella (USDC-PR 209804)

DYKEMA GOSSETT PLLC • 10 S. Wacker Drive, Suite 2300, Chicago, Illinois 60606